POLICY: INTERNET SAFETY

Policy Owner:	School Management
Approved / Last Reviewed:	September 2026
Approved / Last Reviewed by:	Rob Brown
Next Review:	September 2027
Policy basis	

VERSION CONTROL

Version	Date	Author	Notes
1.0			Historic
2.0	September 2026	Rob Brown	Reviewed / Revised - Compliance

Contents

POLICY: INTERNET SAFETY **1**

VERSION CONTROL **1**

INTRODUCTION **2**

RISK **2**

PROVIDING SAFEGUARDING INFORMATION TO PUPILS: **4**

USE OF TECHNOLOGY IN SCHOOL **4**

EARLY YEARS PUPILS (AGED 3-6) 4

LOWER SCHOOL (PUPILS AGED 6-13) 4

UPPER SCHOOL (PUPILS AGED 13-19) 4

STAFF RESPONSIBILITIES: **5**

FURTHER INFORMATION AND SUPPORT **5**

SUPPORT FOR CHILDREN 6

SUPPORT FOR PARENTS 6

MONITORING, AUDIT AND GOVERNANCE 7

INTRODUCTION

Schools and colleges have a statutory responsibility to keep children and young people safe online as well as offline. It is essential that children and young people are safeguarded from potentially harmful and inappropriate online material.

Norwich Steiner School is committed to providing a safe learning environment for its pupils. This policy outlines and describes our approach to information and communications technology (ICT) and online safety in the school. It reflects the school's ethos and curriculum and therefore takes account of the ages and developmental stages of pupils across the school. The policy forms part of our overarching safeguarding approach and should be read alongside the school's mobile phone and electronic devices policy, anti-bullying policy, safeguarding and child protection policy, the curriculum policy and the internet safety agreement.

An effective whole school approach to online safety empowers us to protect and educate pupils and staff in their use of technology and establishes mechanisms to identify, intervene in and escalate any concerns where appropriate.

RISK

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content. For example- pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and exploitation including adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g., Consensual and non-consensual sharing of nudes and semi-nudes and/ or pornography, sharing other explicit images and online bullying; and

- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

In order for us to maintain the welfare of pupils and to create a safe work environment, Norwich Steiner School work to do all that they can to limit exposure to the above risks. A large part of this process is ensuring that the school has appropriate filtering and monitoring in place.

Filtering is a preventative measure that protects pupils from being able to access inappropriate, illegal and potentially harmful content online by identifying and blocking specific web links and content.

Monitoring is reactive and can be both manually and technically managed. Manual monitoring may involve the teacher viewing pupil's screen as they walk around the classroom. Whereas technical monitoring relies. On software being installed on devices that can view individual activity and sends alerts/ reports to nominated safeguarding staff if a pupil accesses or tries to access inappropriate, illegal or harmful content.

In order to meet the government standards and statutory advice and to protect our pupils online, we have invested in a filtering and monitoring system through a company called 'Securly'. Securly are also a member of the Internet Watch Foundation (IWF).

The Department for Education (DfE) have produced a set of filtering and monitoring standards which states that school and colleges should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring systems at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

Technology, risks and harm related to it evolve and are rapidly changing. The designated safeguarding leads (DSL's) in the school hold overall responsibility for meeting the government standards on filtering and monitoring and will review the school's filtering and monitoring provision at least annually.

The Lead DSL is also responsible for any safeguarding and child protection concerns that are identified through monitoring.

We are aware that many children have unlimited and often unrestricted access to the internet through their mobile phones. As a result, we are also aware that some pupils may be at risk at risk of and exposed to inappropriate and harmful content outside of school hours.

Parents play a critical role in ensuring that their children understand that their children need to use the internet and their devices in a safe and appropriate way. We work closely with parents to ensure that they have up to date information in order to help keep their children safe. We help parents understand these issues through parent's evenings, newsletters and e-safety bulletins. Parents are encouraged to support the school in promoting good online safety practice and to support their children in following school policies. The DSL's act as a point of contact in school and source of information for parents.

PROVIDING SAFEGUARDING INFORMATION TO PUPILS:

We provide safeguarding information and guidance directly to the pupils across the school. Kindergarten and younger school pupils are provided with safety messages through specifically designed developmentally appropriate narratives and the teachers address any issues or questions that arise in an age-appropriate way. From class 5, pupils receive information and guidance via the RSHE curriculum, in sponsor and global issue lessons and again teachers address any questions as they arrive.

USE OF TECHNOLOGY IN SCHOOL

We have a strict mobile phone policy (see separate mobile phone policy) and through the implementation of this and the associated sanctions the school ensures that they are creating and maintaining a safe environment.

Mobile phones that are brought onto school site are switched off before pupils enter the school sight and are placed in a locked box which is kept in the school office until the end of the school day. It is for this reason that the risk of pupils accessing harmful or illegal content whilst in school is low.

Early years pupils (aged 3-6)

No electronic devices or technology is used in the kindergarten. Children do not bring devices into school. It is therefore very unlikely and extremely low risk that pupils would access any harmful or illegal material online in school.

Lower school (pupils aged 6-13)

Electronic devices and/ or computers are not used in lower school and any mobile phone that is brought into school is switched off and kept in a locked box in the school office until the end of the school day. The risk of these pupils accessing harmful or illegal material whilst in school is therefore low.

Upper school (pupils aged 13-19)

Pupils are expected to switch off their mobile phones before coming onto school site and are expected to place their mobile phone in a locked box in the office until the end of the school day. For this reason and that mobile phone use in school is strictly prohibited, the risk of pupils accessing harmful and/ or inappropriate content using their mobile phones in school remains low. When pupils start their NZCSE, they are able to access laptops and use either their own personal device or a school laptop. They are only permitted to use these for work and research purposes. As the school has a secure filtering and monitoring system in place which blocks harmful and inappropriate websites as well as sending alerts to the DSL's if something concerning is accessed or access is attempted, the chances of pupils accessing harmful/ illegal or inappropriate content through such devices is also low.

Computer use is monitored through both manual and technological checks using the schools filtering and monitoring system.

Where pupils are found to have deleted their search history or where they have tried to access apps that they have not been given permission to access, the class guardian or DSL will speak with them and explain that they are in breach of their computer user agreement with the school. Staff will discuss the issues of trust and the implications of mistrust regarding computer use. In cases of concern, pupils be prevented from using computers for a defined period of time or they may only be able to use them for specific tasks where staff can see their screen.

The school continues to review their approach to filtering and monitoring as well as internet safety, taking into account statutory guidance and changes to risk whilst remaining conscious to the fact that over-blocking may adversely affect pupil's educational experience and ability to manage their own online safety outside of school.

STAFF RESPONSIBILITIES:

Staff acknowledge that children from kindergarten upwards will be accessing devices and content outside of school and are alert to any areas of concern which are addressed with parents or the safeguarding team as appropriate.

All staff have an awareness and understanding of online safety, including radicalisation, as part of wider safeguarding in the school, and this is reflected in safeguarding training. Upper school staff are alert to pupils' online activity in class and the DSLs act as a source of information for all staff. Training is provided annually for all staff, and the DSL has also undertaken NSPCC training in keeping children safe online, sexual harassment, peer on peer abuse, and child sexual exploitation and abuse.

FURTHER INFORMATION AND SUPPORT

- Childnet
- Educate against hate provides practical advice and support on protecting children from extremism and radicalisation
- London grid for learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- Searching, screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West grid for learning provides advice on all aspects of a school or college's online safety arrangements

- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq

- UK Council for Internet Safety have provided advice on, and an Online safety audit tool to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring

- Department for Digital, Culture, Media & Sport DCMS Online safety guidance provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk.

- Department for Digital, Culture, Media & Sport (DCMS) A business guide for protecting children provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to protect children's personal data, ensure content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse.

Support for children

- Childline for free and confidential advice

- UK safer internet centre to report and remove harmful online content

- CEOP for advice on making a report about online abuse

Support for Parents

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support

- Common sense media provide independent reviews, age ratings, & other information about all types of media for children and their parents

- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying

- Government advice about security and privacy settings, blocking unsuitable content, and parental controls

- Internet matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world

- London grid for learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

- Stop it now resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- Net aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parent zone provides help for parents and carers on how to keep their children safe online
- UK safer internet centre provide tips, advice, guides and other resources to help keep children safe online

MONITORING, AUDIT AND GOVERNANCE

This policy belongs to Norwich Steiner School, which is the operational name for the Charity the Norfolk Initiative Steiner School, registered charity number 1099377, company number 4815492

Compliance is monitored through internal audits, policy review as part of self-evaluation, and annual reporting to Trustees on concessions awarded, value, and any compliance issues.